1. At a module having at least one measurable aspect, the module being communicatively connectable to a verification module that can verify the authenticity of assertions formulated at other modules, a method for providing information that can be used to securely verify measurable aspects of the module, the method comprising:

an act of accessing an indication that one or more measurable aspects of the module's configuration are to be verified;

an act of formulating an assertion that can be used to verify that the module is configured in accordance with the one or more measurable aspects; and

an act of sending the formulated assertion for verification.

2. The method as recited in claim 1, further comprising:

an act of sending a request to access a resource of a providing module prior to accessing the indication that one or more measurable aspects of the module's configuration are to be verified

3. The method as recited in claim 1, further comprising:

an act of receiving a request for proof that the module is appropriately configured to issue challenges to a requesting module, the request being received prior to accessing the indication that one or more measurable aspects of the module's configuration are to be verified.

4. The method as recited in claim 1, wherein the indication is administrative policies associated with the resource.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

5. The method as recited in claim 1, wherein the indication is a message from the verification module.

6. The method as recited in claim 1, wherein the indication is a request for information that allows the values of one or more measurable aspects of the module's configuration to be verified.

7. The method as recited in claim 6, wherein the request for information is a request for values associated with one or more of an assembly, a SEE application, a hardware component, a platform, an environment variable, a call stack, and a data stream.

8. The method as recited in claim 6, wherein the request for information is a request for the values of the one or more measurable aspects.

9. The method as recited in claim 8, wherein the request for the values of the one or more measurable aspects is a request for the identity of one or more portions of executable instructions at the requester.

10. The method as recited in claim 8, wherein the request for the values of the one or more measurable aspects is a request for the values of the one or more measurable aspects of an execution environment at the requester.

11. The method as recited in claim 6, wherein the request is a request for a representation of the values of the one or more measurable aspects.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

12. The method as recited in claim 11, wherein the request for a representation of the values of the one or more measurable aspects is a request for a digest of the one or more measurable aspects.

13. The method as recited in claim 1, wherein the assertion is an assertion that the module is appropriately configured for accessing a resource of a providing module.

14. The method as recited in claim 1, wherein the assertion is an assertion that the module is appropriately configured for issuing challenges to a requesting module.

15. The method as recited in claim 1, wherein the assertion is formulated proof that can be used to verify the identity of one or more portions of executable instructions.

16. The method as recited in claim 1, wherein the assertion is formulated proof that can be used to verify one or more measurable aspects of an execution environment.

17. The method as recited in claim 16, wherein the formulating proof is formulated proof that the module is to execute in a compartmentalized environment.

18. The method as recited in claim 16, wherein the formulated proof of is formulated proof that the module has access to one or more of an assembly, a SEE application, a hardware component, a platform, an environment variable, a call stack, or a data stream.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

19. The method as recited in claim 1, wherein the assertion is a formulated representation of the values of the one or more measurable aspects.

20. The method as recited in claim 19, wherein the formulated representation is a digest representing the values of the one or more measurable aspects.

21. The method as recited in claim 1, wherein the assertion is formulated proof that indicates at least one of compliance with one or more required policies or a providing module, that the module is not a virus, and that the module is not an intruder.

22. The method as recited in claim 1, wherein the assertion is formulated proof that the module is configured in accordance with at least one pre-determined configuration.

23. The method as recited in claim 1, further comprising:

an act of digitally signing the formulated proof .

24 The method as recited in claim 23, wherein the proof is signed using a private key that can be validated by a group public key also able to validate at least one other private key.

25. The method as recited in claim 23, wherein the proof is signed using a per-machine that identifies the module.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

26. The method as recited in claim 23, wherein the proof is signed using a zero knowledge algorithm.

27. The method as recited in claim 23, wherein the proof is signed using a hardware-based key.

28. The method as recited in claim 23, wherein the proof is signed using a communication channel key.

29. The method as recited in claim 23, wherein the act of digitally signing the formulated proof comprises an act of digitally signing data from one or more identified code regions within in the module.

30. The method as recited in claim 1, wherein the act of sending the formulated assertion to the verification module comprises sending the formulated assertion to a token service.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

31. The method as recited in claim 1, further comprising:

an act of receiving a token that represents proof that one or more measurable aspects have been verified.

32. The method as recited in claim 1, further comprising:

an act of downloading a list of one or more configurations that have been pre-determined to be appropriate for accessing a resource.

33. At a module communicatively connectable to another module that can send assertions to the module, a method for verifying that the other module is configured in accordance with one or more measurable aspects, the method comprising:

an act of providing an indication that one or more measurable aspects of the other module's configuration are to be verified;

an act of receiving an assertion that can be used to verify that the other module is configured in accordance with the one or more measurable aspects; and

an act of verifying the assertion.

34. The method as recited in claim 33, further comprising:

an act of receiving a request to access a resource of the module prior to providing the indication of the one or more measurable aspects of the other module's configuration that are to be verified.

35. The method as recited in claim 33, further comprising:

an act of sending a request for proof that the other module is appropriately configured to issue challenges to the module, the request being sent prior providing the indication of the one or more measurable aspects of the other module's configuration that are to be verified.

36. The method as recited in claim 33, wherein the indication is a challenge that requests information that allows the one or more measurable aspects to be verified.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

37. The method as recited in claim 36, wherein the challenge requests proof of the values of one or more measurable aspects.

38. The method as recited in claim 37, wherein the challenge requests a representation of the values of the one or more measurable aspects.

39. The method as recited in claim 38, wherein the challenge requests a digest of the one or more measurable aspects.

40. The method as recited in claim 36, wherein the challenge requests proof of the identity of one or more portions of executable instructions.

41. The method as recited in claim 36, wherein the challenge requests proof an execution environment.

42. The method as recited in claim 33, wherein the assertion includes the identity of one or more portions of executable instructions.

43. The method as recited in claim 33, wherein the assertion includes the values of one or more measurable aspects of an execution environment.

44. The method as recited in claim 43, wherein the assertion indicates that the other module has access to one or more of an assembly, a SEE application, a hardware component, a platform, an environment variable, a call stack, and a data stream.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

45. The method as recited in claim 43, wherein the assertion is a representation of the values of one or more measurable aspects of the requester.

46. The method as recited in claim 45, wherein the assertion is a digest of the values of one or more measurable aspects of the requester.

47. The method as recited in claim 33, wherein the assertion indicates that the other module is executing in a compartmentalized resource.

48. The method as recited in claim 33, wherein the assertion indicates at least one of compliance with one or more administrative policies, that the other module is certified to access a resource of the module, that the other module is not a virus, that the other module is not infected with a virus, that the other module is not an intruder, and that the other module is appropriately configured to issue challenges to the module.

49. The method as recited in claim 33, wherein the assertion is a token issued from a token service.

50. The method as recited in claim 33, wherein the assertion indicates that the other module is configured in accordance with at least one pre-determined configuration.

51. The method as recited in claim 33, wherein the assertion is verified using a group public key that corresponds to a plurality of private keys.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

52. The method as recited in claim 33, wherein the assertion is verified using a zero knowledge algorithm.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

53. A computer program product for use in a computing system with a module having at least one measurable aspect, the module being communicatively connectable to a verification module that can verify the authenticity of assertions formulated at other modules, the computer program product for implementing a method for providing information that can be used to securely verify measurable aspects of the module, the computer program product comprising one or more computer-readable media having stored thereon computer-executable instructions that, when executed by a processed, cause the computer system to perform the following:

access an indication that one or more measurable aspects of the module's configuration are to be verified;

formulate an assertion that can be used to verify that the module is configured in accordance with the one or more measurable aspects; and

sending the formulated assertion for verification.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

54. A computer program product for use in a computing system with a module communicatively connectable to another module that can send assertions to the module, the computer program product for implementing a method for verifying that the other module is configured in accordance with one or more measurable aspects, the computer program product comprising one or more computer-readable media having stored thereon computer-executable instructions that, when executed by a processed, cause the computer system to perform the following:

provide an indication that one or more measurable aspects of the other module's configuration are to be verified;

receive an assertion that can be used to verify that the other module is configured in accordance with the one or more measurable aspects; and

verify the assertion.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111